REMARKS

The Examiner rejects Claims 1, 3-4, 9, 11-12, 17, and 19-20 under 35 U.S.C. 102(b) as being anticipated by Warrender ("Detecting Intrusions Using System Calls: Alternate Data Models" IEEE Computer Society, Symposium on Security and Privacy, 1999, 133-145). Applicant respectfully disagrees with this rejection, especially in view of the amendments made hereinabove.

For example, the Examiner relies on the following excerpt from Warrender to make a prior art showing of applicant's claimed "receiving an exemplary set of system calls that includes ... possibly negative examples of invalid system calls" (see all independent claims).

> "In 1996, Forrest and others introduced a simple intrusion detection method based on monitoring the system calls used by active, privileged processes [4]. Each process is represented by its *trace*—the ordered list of system calls used by that process from the beginning of its execution to the end. This work showed that a program's normal behavior could be characterized by local patterns in its traces, and deviations from these patterns could be used to identify security violations of an executing process. There are two important characteristics of the approach introduced in [4]. First, it identifies a simple observable (short sequences of system calls) that distinguishes between normal and intrusive behavior." (see Section 1.0, Line 2-13)

Such excerpt and the remaining Warrender reference, however, merely suggest monitoring a program's normal behavior. There is simply no disclosure, teaching or even suggestion of any sort of "receiving an exemplary set of system calls that includes ... possibly negative examples of invalid system calls." Only applicant teaches and claims such a technique capable of receiving possibly negative examples of invalid system calls, as claimed, for the specific purpose of constructing rules, "wherein the set of rules covers all positive examples in the exemplary set of system calls without covering negative examples" (see all independent claims). Since Warrender does not receive possibly negative examples of invalid system calls, it is incapable of generating rules that do not cover the same.

The Examiner is reminded that a claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described in a single prior art reference. *Verdegaal Bros. v. Union Oil Co. Of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). Moreover, the identical invention must be shown in as complete detail as contained in the claim. *Richardson v. Suzuki Motor Co.*868 F.2d 1226, 1236, 9USPQ2d 1913, 1920 (Fed. Cir. 1989). The elements must be arranged as required by the claim. This criterion has simply not been met by the Warrender reference.

Despite this clear distinction already present in the claims and in the spirit of expediting the prosecution of the present application, applicant now claims in each of the independent claims the subject matter of Claims 2, 10, and 18 below:

> "wherein the objective function additionally seeks to minimize the number of privileged system calls covered by the rule" (see this or similar language in each of the independent claims).

The Examiner rejected the subject matter of Claims 2, 10, and 18 under 35 U.S.C. 103(a) as being unpatentable over Warrender ("Detecting Intrusions Using System Calls: Alternate Data Models" IEEE Computer Society, Symposium on Security and Privacy, 1999, 133-145), in view of Ko ("Automated Detection of Vulnerabilities in Privileged Programs by Executing Monitoring", 1994). Applicant respectfully disagrees with this rejection.

For example, the Examiner relies on the following excerpt from Ko to make a prior art showing of applicant's claimed "wherein the objective function additionally seeks to minimize the number of privileged system calls covered by the rule" (see all independent claims).

> "Although our approach is not complete, we strongly believe that by appropriately restricting the behavior of privileged programs, the chance in these programs can be greatly reduced" (see Section 8.0, Lines 30-33)

Such excerpt and the remaining Ko reference, however, merely suggest restricting the behavior of privileged programs. There is simply no disclosure, teaching or even suggestion of any

sort of handling privileged system calls, let alone "minimize[ing] the number of privileged system calls covered by the rule," as claimed. Only applicant teaches and claims such a technique for enhancing the resultant intrusion detection.

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure. *In re Vaeck,* 947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

Applicant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all the claim limitations. A notice of allowance or a specific prior art showing of such claimed features, in combination with the remaining claim limitations, is respectfully requested.

Applicant further notes that the Examiner's application of the prior art to the dependent claims is also replete with deficiencies. Just by way of example, with respect to Claims 8, 16, and 24, the Examiner rejects the same under 35 U.S.C. 103(a) as being unpatentable over Warrender ("Detecting Intrusions Using System Calls: Alternate Data Models" IEEE Computer Society, Symposium on Security and Privacy, 1999, 133-145), in view of Cohen (Patent Number 5,481,650). Applicant respectfully disagrees with this rejection.

For example, the Examiner relies on Figure 3 and the following excerpt from Cohen to make a prior art showing of applicant's claimed "constructing a Horn clause for the positive example by iterating through a subsumption lattice, starting from a most general possible clause and proceeding to a most specific clause for the positive example, and selecting a Horn clause that maximizes the objective function without covering any negative examples; adding the Horn clause to the set of rules in the valid behavior specification; and removing other positive examples covered by the Horn

clause from the exemplary set of system calls, so subsequently selected Horn clauses do not have to cover the other positive examples" (see Claims 8, 16, and 24).

> "The training data contains both positive and negative examples. In one embodiment of the invention, the hypothesis generation proceeds by calculating the "information gain" with respect to such data for each of a first series of derived Horn clauses, choosing the clause with the highest information gain and, if the chosen clause covers negative examples, repeating such calculating and choosing steps for successive levels of Horn clauses until a clause results that does not cover negative examples, or that covers only an acceptably small number of negative examples. Such clause is added to the hypothesis and the positive examples covered by the clause are removed. The process is repeated until substantially all positive examples are eliminated. The clauses forming the hypothesis can then be used to evaluate whether examples in new data are positive or negative examples." (see Col. 2, line 59 - Col. 3, line 7)

The mere mention of hypothesis generation involving Horn clauses, as noted in the above excerpt and the remaining Cohen reference, simply does not rise to the level of specificity of applicant's claims. In particular, there is simply no disclosure, teaching or even suggestion of any sort of "constructing a Horn clause for the positive example by iterating through a subsumption lattice, starting from a most general possible clause and proceeding to a most specific clause for the positive example, and selecting a Horn clause that maximizes the objective function without covering any negative examples; adding the Horn clause to the set of rules in the valid behavior specification; and removing other positive examples covered by the Horn clause from the exemplary set of system calls, so subsequently selected Horn clauses do not have to cover the other positive examples" (emphasis added - see Claims 8, 16, and 24).

Applicant again respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all the claim limitations. Again, a notice of allowance or a specific prior art showing of such claimed features, in combination with the remaining claim limitations, is respectfully requested.

Still yet, applicant brings to the Examiner's attention the subject matter of new Claims 25-27 below, which is deemed to be novel:

"wherein the objective function includes: $f_h = e_h - (g_h + p_h + c_h)$, where:

$g_h$ = the generality of clause $h$;

$p_h$ = the privilege of clause $h$;

$c_h$ = the length of the clause $h$; and

$e_h$ = the explanation power" (see Claim 25);

"wherein the values $g_h$ and $p_h$ are normalized to range from 1 to the total number of valid traces" (see Claim 26); and

"wherein the value $f$ is set to favor short, low-privilege, and low-generality clauses while explaining examples in many traces" (see Claim 27).

Thus, all of the independent claims are deemed allowable. Moreover, the remaining dependent claims are further deemed allowable, in view of their dependence on such independent claims.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 505-5100. The Commissioner is authorized to charge any additional fees or credit any overpayment to Deposit Account No. 50-1351 (Order No. NAI1P253/00.121.01).

Respectfully submitted,
Zilka-Kotab, PC.

Kevin J. Zilka
Registration No. 41,429

P.O. Box 721120
San Jose, CA 95172-1120
408-505-5100